



CDVAOHI  
HIPAA

General Implementation Plan

**California**  
**Department of Veterans Affairs**  
**Office of HIPAA Implementation**  
**(CDVAOHI)**

**HIPAA**  
**General Implementation Plan**  
**Special Project**  
***FINAL NARRATIVE***

“...If the State is not compliant with HIPAA regulations, federal funding for health care delivery programs may be lost and other financial penalties may be imposed.  
Inadequate implementation could result in increased General Fund costs and hinder  
The delivery of and payment for health care...”

CA Department of Finance  
2001- 2002  
Governor's Budget Summary (Excerpt)

---

**Leon E. Tuttle**  
**Interim Secretary**

**Ivann E. Greene, AICP**  
**Agency HIPAA Project Manager**  
**CDVA Office of HIPAA Implementation**

## **Table of Contents**

Table of Contents	2
Preface	3
Legislature	3
Privacy	4
Security	4
Transactions and Code Sets	5
Sanctions for HIPAA Non-Compliance	5
Financial Penalties for HIPAA Non-Compliance	5
The CDVA Office of HIPAA Implementation (CDVAOHI)	5
CDVA HIPAA Project Milestones	6
Project Methodology	6
Implementation Strategy	7
Privacy	7
1. CDVAOHI Major Deliverables	7
2. Assessment Result	7
3. Approach	8
4. Resources Needed	9
5. Critical Success Factors	9
Transaction and Code Sets	10
Security	10
1. Major Deliverables	10
2. Issues and Obstacles to Overcome	10
3. Approach	11
4. Resources Needed	12
5. Critical Success Factors	12
References	14

## **Preface**

CDVA must comply with the Health Insurance Portability Accountability Act (HIPAA) of 1996, as CDVA is a covered entity under the HIPAA regulations. CDVA must institute new business practices and modify its systems relating to clients' health claims, encounter data, eligibility, enrollment and dis-enrollment, remittance advice, premium payments, and claim status.

HIPAA's privacy and security rules will fundamentally change the way CDVA deals with its many business partners and providers. CDVA will have to establish new policies and procedures for privacy, confidentiality, and security for Protected Health Information (PHI).

The HIPAA Privacy compliance deadline was April 2003, and the Transactions and Code Sets compliance deadline is October 2003. System changes must be ready for testing in April 2003. CDVA established a formal project management structure for the three areas in which the federal government has already issued proposed HIPAA regulations:

- Privacy
- Transactions and Code Sets
- Security

Because of internal transitional management matters, CDVA's HIPAA program has not been a management priority. Complete HIPAA assessments and gap analyses for all parts of the project are scheduled to be contracted-out in March of 2003 – one month before the mandated compliance period under the privacy rule. In September of 2002, a new Agency Coordinator was appointed who reinvented and rejuvenated CDVA's plan of action. As a result of this new "positive attitude", federal mandates under HIPAA have been re-reviewed and re-explained in detail to CDVA's executive staff. In January of 2003, Undersecretary Tom Kraus assumed executive sponsorship of CDVA's HIPAA project.

## **Legislature**

Under Section 17, the legislature appropriated \$134,000 to CDVA for HIPAA implementation. CDVA must optimize its appropriation by phasing in the three components. The estimated cost of the initial HIPAA assessment will be between \$100,000 and \$119,000, with the remaining amount being devoted to training CDVA staff and project support equipment purchases. **(See Exhibit 1, CA Legislative Action – CDVA HIPAA Appropriation Enabling Legislation, and Exhibit 2, CalOHI Assessment Funding Request w/Denial Justification)**

Security issues related to HIPAA will require an additional appropriation from the legislature or a Budget Change Proposal to support CDVA's compliance effort.

Major project costs involve:

- Revising and developing policies, procedures and various forms
- Training all relevant CDVA staff, some possible 500 individuals, on new privacy policies, procedures and forms
- Remediating information systems requiring an unknown number of man-hours
- Implementing a security infrastructure that fully complies with federal HIPAA regulations.

Among the tasks facing CDVA for compliance and implementation are:

- Development of numerous policies and procedures
- Systems to track the use and disclosure of PHI
- Establishment of a CDVA Privacy Program and appointment of a Chief Privacy Officer **(See Exhibit 3, CDVA Draft Specifications for a Chief Privacy Officer)**
- Changes in and creation of client authorization forms and notification of client rights
- Staff training to include a documentation log for auditing purposes
- A determination of the relationships among the various homes and HQ programs and what level of consent or release of information is needed to communicate accordingly.

### **Privacy**

The privacy rule requires that the entire CDVA workforce be informed of policies regarding the disclosure of PHI and the possible penalties for non-compliance. Everyone in CDVA, inclusive of senior management, may need to be trained regarding HIPAA's privacy rule prior to the April 2003 implementation date of the privacy component. **(See Exhibit 4, HIPAA Total Workforce Awareness Statement)**

Privacy is defined as controlling who is authorized to access information (the right of individuals to keep information about themselves from being disclosed).

### **Security**

Security is defined as the ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss.

Although the final security regulations have yet to be promulgated, the federal government has indicated that entities must still comply with statutory obligations even without written regulations.

## **Transactions and Code Sets**

This portion of HIPAA requires national uniform transactions and codes for the electronic exchange of information.

Examples of business processes covered by HIPAA include health claims and encounter data, eligibility, enrollment and disenrollment, a health plan, health care payment and remittance advice, health plan premium payments and claim status.

## **Sanctions for HIPAA Non-compliance**

Implications for organizations who **do not** comply could range from increased operating costs, loss of accreditation (JCAHO, NCQA, etc.), imprisonment for its officers, to litigation damages, increased capital costs associated with “late” compliance efforts, and/or public exposure could lead to loss of market share.

## **Financial Penalties for HIPAA Non-compliance**

Non-compliance may also result in civil penalties of \$100 with a maximum of \$25,000 per year per incident. Unauthorized disclosure or misuse of patient information may result in criminal penalties of up to \$250,000 and prison time of up to ten (10) years. Penalties may apply to the individual violator, but they may also apply to the organization or even to its officers.

In addition, the federal government has required that all state Medicaid agencies become HIPAA compliant. CDVA receives a substantial amount of Medicaid funds. CDVA could potentially lose thousands of dollars in Medicaid funding if it does not meet HIPAA compliance mandates.

Documentation of “**due diligence**” could relieve CDVA of any penalties. CDVA, therefore, must make a **concerted and documented effort** toward compliance or face embarrassing consequences.

## **The CDVA Office of HIPAA Implementation (CDVAOHI)**

The CA Department of Veterans Affairs Office of HIPAA Implementation is comprised of key CDVA staff whose purpose is to insure that CDVA is HIPAA compliant. Personnel from the following CDVA components make up CDVAOHI:

- Executive Office – Executive Steering Committee
- Veterans Homes Division (VHC)
- Information Services Division (ISD)
- Legal Division (LD)
- Financial Management Division (FMD)
- Farm and Home Loan Purchases Division (FHLPD)
- Veteran Services (VSD)

Members of CDVAOHI are working together to improve the understanding of and compliance with the HIPAA. **(See Exhibit 5, CDVAOHI Org Chart, and Exhibit 6, CDVAOHI Team Member Roles and Responsibilities Agreement)** The Agency Coordinator has requested that all CDVA staff begin logging their time allocated to the HIPAA project by using a specialized cost allocation time sheet. This specialized time sheet will be distributed to all members of the CDVAOHI team. **(See Exhibit 7, Project Cost Allocation Timesheet)**

### **CCDVA HIPAA Project Major Milestones**

Completed HIPAA assessment and gap analysis for Privacy, Security, Transaction and Code Sets	July 2003
Revise Privacy and Security business practices	April 2003
Transaction and Code Set system software finalization	March 2003
Internal CDVA Staff Training (on-going)	April/May 2003
Privacy regulations effective	April 2003*
Commence Transaction and Code Set system testing	March 2003
Commence security infrastructure implementation	December 2003
Transaction and Code Set regulation effective	October 2003

**\*Note** – April 14, 2003 was the deadline for Privacy compliance.

### **Project Methodology**

CDVA has chartered a project to work on the three areas for which the federal government has already issued proposed HIPAA regulations: Privacy, Transactions and Code Sets, and Security. The Security Rule has yet to be finalized by the federal government.

It is the intention of CDVA to use a phased implementation approach for each portion of the project. The project phases will be:

1. Planning and Assessment
2. Development; and
3. Implementation and Acceptance

The Privacy sub-project is in the Planning and Assessment phase. The Transaction and Code Sets sub-project is in the Development Phase. The Security sub-project is in the Planning and Assessment Phase.

The Privacy sub-project will focus on business processes to ensure the privacy of private health information (PHI).

CDVA's Information Services Unit (ISU) has coordinated the Transactions and Code Sets sub-project with Meditech, CDVA's contracted software partner. CDVA has been assured that its transaction and coding information software will be HIPAA compliant. As of this report, however, system software confirmation has been verified, and "final" transaction code set testing schedule been performed with results provided to CDVA.

## **Implementation Strategy**

### **Privacy**

#### **1. CDVAOHI Major Deliverables**

- A. Policies, procedures and business practices that are aligned with HIPAA regulations and foster HIPAA compliant behavior.
- B. Effective tracking systems and forms that support HIPAA compliance.
- C. HIPAA Privacy training and on-going education and communication provided to all CDVA staff.
- D. CDVA Privacy Program established, tested and implemented agency wide.

#### **2. Assessment Result**

- A. CDVA provided policies and procedures that support HIPAA compliant through:
  - i. building awareness and an understanding among CDVA staff;
  - ii. developing a framework to support the change(s);
  - iii. implementation of HIPAA compliant policies and practices; and
  - iv. re-evaluation of original goals and objectives.
- B. CDVA reviewed and then modified its forms, and created new forms when necessary. In addition, CDVA must defined and developed systems to track the use and disclosure of PHI.
- C. CDVA met the goal of providing HIPAA training to its total workforce by April 14, 2003. Training in policies, procedures and business practice changes resulting from the implementation of HIPAA, will be on going. Training will be deployed in multiple levels addressing the various degrees of staff involvement with PHI.

- D. CDVA is required to “make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.” CDVA has addressed how it will appropriately deal with “minimum necessary” requirements and has defined a plan of action to accomplish it.
- E. CDVA has amended its contract documents with identified business associates to include HIPAA compliant language. CDVA’s Contract Management Unit (CMU) contracts with approximately 1,000 Contractors in one fiscal year. The number of health providers is in excess of 500.

### **3. Approach**

- A. CDVAOHI conducted a thorough assessment of all HIPAA related policies, procedures and business practices; identified how PHI is handled and processed through the various CDVA systems; developed a gap analysis using the CalOHI Implementation Plans; determined the overall business impact to CDVA; and identified all risks associated with no-compliant behaviors and activities.
- B. CDVA has maintained a close working relationship with CalOHI, thus ensuring CDVA’s understanding of legal liabilities, legal responsibilities, and issues and concerns involving the implementation of the HIPAA Privacy requirements.
- C. Provides on-going HIPAA related communications and training to staff. Information has been provided to CDVA business associates in relationship to the work they perform on behalf of CDVA or the services they provide.
- D. Reviewed and revised all CDVA business practices and contracts involving the exchange or handling of client (home residents, CA veterans) information in order to integrate and reflect the new HIPAA requirements.
- E. Developed and implemented a compliance monitoring program which includes effective tracking systems for use and disclosure of PHI; HIPAA compliant forms for authorization, use or release of information; and compliance and enforcement processes that ensure continued HIPAA compliance.
- F. Assessed various divisions and offices’ physical environment to determine the level of safeguards, and to make recommendations on changes that foster HIPAA compliant behavior. Where reasonably necessary, changes are made to reduce or mitigate risks associated with violations to the minimum necessary requirements.



- G. Created an interactive CDVAOHI link with training modules on CDVA's Intranet web page (HIPAA 100).

#### **4. Resources Needed**

- A. Full-time personnel to provide on going oversight, and to conduct periodic assessments inclusive of all work related to policy and procedure review, preemption, business and cost impact(s), and risk assessment.
- B. CDVA's project structure will provide guidance and legal advice for the duration of the project. This should be maintained.
- C. CalOHI is currently developing training modules to provide core HIPAA Privacy training. Beyond CalOHI, CDVA must decide to either engage consultants to provide any further specialized support and direction, or identify a funding base, via BCP, for CDVA staff to receive specialized training so that they can then train other CDVA staff.
- D. Financial resources will be needed to facilitate workshops to develop policy structure and language recommendations. The workshops would draw from staff In CDVA with rich knowledge and expertise in its business functions and practices.

#### **5. Critical Success Factors**

- A. CDVA's HIPAA project will need to have executive management commitment to make the necessary HIPAA related changes. Currently, staff's marginal attitude toward HIPAA may be driven by other operational priorities, rather than a desire to meet the federal mandates as required by HIPAA.
- B. The CDVA HIPAA project will need to have active participation and involvement of selected CDVA staff who represent the Agency's various business and programmatic areas.
- C. CDVA will need to seek and provide the necessary resources and financial means to fully support the project and its objectives as mentioned above.
- D. CDVA will need to have strong commitment toward proactive and effective HIPAA communication, and institute a solid and sustainable staff awareness and training program.

- E. CDVA will need to enhance its Communication Plan to promulgate requirements, and new policies and procedures under the HIPAA rules.

### **Transactions and Code Sets**

CDVA's Information Services Division (ISD) has performed testing on the new Meditech software features, which address HIPAA transactions and code standards. The testing schedule outlined in the extension request is currently in effect. Further, CDVA has configured the reimbursement system to create the 4010 claim files. Meditech, ISD and CDVA Reimbursement staffs have met all relevant parameters. CDVA will meet the Transaction and Code Sets deadline.

### **Security**

#### **1. Major Deliverables**

- A. CDVA will assess, design, implement, and manage an Information Security Program that addresses the core components of a security program:
  - Policies
  - Standards
  - Procedures
  - Processes
  - Organization
  - Technology

#### **2. Issues and Obstacles to Overcome**

- A. CDVA's information system architectures will need to be either restructured or enhanced to reflect mandates under HIPAA Security rules and regulations.
- B. Due to budget constraints, CDVA does not have sufficient funding, or a dedicated budget to address all aspects of the HIPAA mandate for information security.
- C. The HIPAA security rule has not been released for final review as of this report. Nevertheless, HIPAA's statutory security provisions are currently in effect.
- D. CDVA will need to conduct an information security assessment and evaluation because specific risks and threats have yet to be identified.

- E. CDVA will need to perform an independent system security certification at the completion of the project to confirm and verify that adequate security controls are in place.

### **3. Approach**

- A. Security Assessment – Perform a security assessment and evaluation to identify critical asset threat profiles, identify infrastructure vulnerabilities, develop security strategies and plans.
- B. Security Consultant – CDVA must either identify competent in-house security personnel who are familiar with information security requirements, or hire a security consultant to provide expertise and guidance throughout the security review process. This security expertise must be able to design, implement, and impart knowledge of security administration, practices, and implementation procedures to CDVA staff. In light of the state's budgetary crisis, the latter may not be a viable option however.
- C. Security Technology – Design and build the security infrastructure in a phased approach of network security, system security, application security and data security.
- D. Information Security Program – Build an information security program that establishes the following key objectives:
- Establish information risk management objectives
  - Identify information assets needing protection, and what they need protection from
  - Develop or refine information security policies, standards, procedures, and processes.
  - Establish or refine the governance for information security
  - Build agency security architecture
  - Define and build agency security infrastructure
  - Develop, implement, and maintain effective information security remedies
- E. Leverage, if at all possible, existing state security contracts – Whenever possible and feasible, use existing state contracts in order to avoid time and expenses associated with the procurement process.
- F. If feasible, hire a third-party certification consultant – Hire an independent contractor to certify that security requirements have been attained. This can be done through item E above.

#### **4. Resources Needed**

- A. Security consulting – A consulting firm may be needed to provide expertise and guidance throughout the project.
- B. Financial Support – Identify and obtain funding (internal or external)
- C. ISD Staff – Assign existing staff and acquire additional staff to implement technical security controls into systems and applications.
- D. Programmatic and Divisional Staff – Assign representatives from affected program or division areas to participate in the development and implementation of security policies, practices, and procedures.
- E. Contract Management – Procure security contractors to design, implement, and impart knowledge of technical security hardware to CDVA staff. Actually engaging DVBE's rather than specifying a "good faith effort" would should be an incentive.
- F. Legal Support – Karla Broussard-Boyd, of the CDVA Legal Division has been assigned to review any and all legal matters relating to CDVA's HIPAA effort. CDVA's Legal Division would oversee the development and implementation of "chain-of-trust" Agreements with business partners for exchanging sensitive information.

#### **5. Critical Success Factors**

- A. Support of the Secretariat – Executive support will be critical for what can be accomplished, how much it will cost, and the security problems, and make recommendations both strategically and tactically.
- B. Adequate funding – Obtaining adequate funding to support the project will be a determining factor as to how far we can proceed with implementation.
- C. CDVA security blueprint – Developing a flexible security architecture and infrastructure that includes HIPAA elements in the early stages.
- D. Training – Developing and implementing quality training for CDVA workforce.

- E. Communication Plan – CDVA must develop a Communication Plan to promulgate the requirements and directives of HIPAA and communication.

**END**

---

## **References**

- **California Office of HIPAA Implementation**  
Burt Cohen, Director  
Alex Kam, Chief of Operations  
Ruth Jacobs, Agency Liaison  
Alan Zamansky, Agency Liaison  
<http://www.calohi.ca.gov>
- **New Hampshire Vermont Strategic HIPAA Implementation Plan**  
Greg Farnum, Co-Chair - NHVSHIP/VT Hospitals  
Kathy Bizarro, Co-Chair - NHVSHIP/VT Hospitals  
<http://www.nhvship.org/index.htm>
- **Oregon Department of Veterans Affairs**  
Charles Gehley, Director  
<http://www.hr.state.or.us/hipaa/welcome.html>
- **CA Department of Health Services**  
Judy Gelein  
Michelle Marks  
Julie Dittman  
<http://www.dhs.ca.gov/hipaa/>
- **HIPAA Security Summit Guidelines 2000**

## **Exhibits**

- Exhibit 1 - CA Legislative Action CDVA HIPAA Appropriation - Enabling Language
- Exhibit 2 - CalOHI Assessment Funding Request w/Denial Justification (email)
- Exhibit 3 - CDVA Draft Specifications for a Chief Privacy Officer
- Exhibit 4 - HIPAA "Total Workforce Awareness" Statement
- Exhibit 5 - CDVAOHI Organization Chart
- Exhibit 6 - CDVAOHI Team Member Roles and Responsibilities Agreement
- Exhibit 7 - CDVAOHI Project Cost Allocation Timesheet
- Exhibit 8 - MEDITECH Description of Services with CDVA

H:HIPAA FINAL IMPLEMENTATION PLAN. CDVAHIT